The Ultimate Guide to Network Monitoring

GARLAND TECHNOLOGY

See every bit, byte, and packet®

Introduction

Because network monitoring is such a broad topic with so many critical components, we decided to publish this guide that consolidates everything you need to know as you scale your network to meet modern business demands.

From monitoring basics to industry best practices, infrastructure concerns and scaling network speeds, Garland's goal is to share our knowledge to help build the better networks of tomorrow, and be your reference when you have network monitoring questions.

Table of Contents

Back to the Network Monitoring Basics

What Is Network Monitoring?

Network monitoring is far from a new topic. However, with so many new networking trends and applications demanding attention it's easy to lose focus on network monitoring despite the fact that it's so critical to long-term business success.

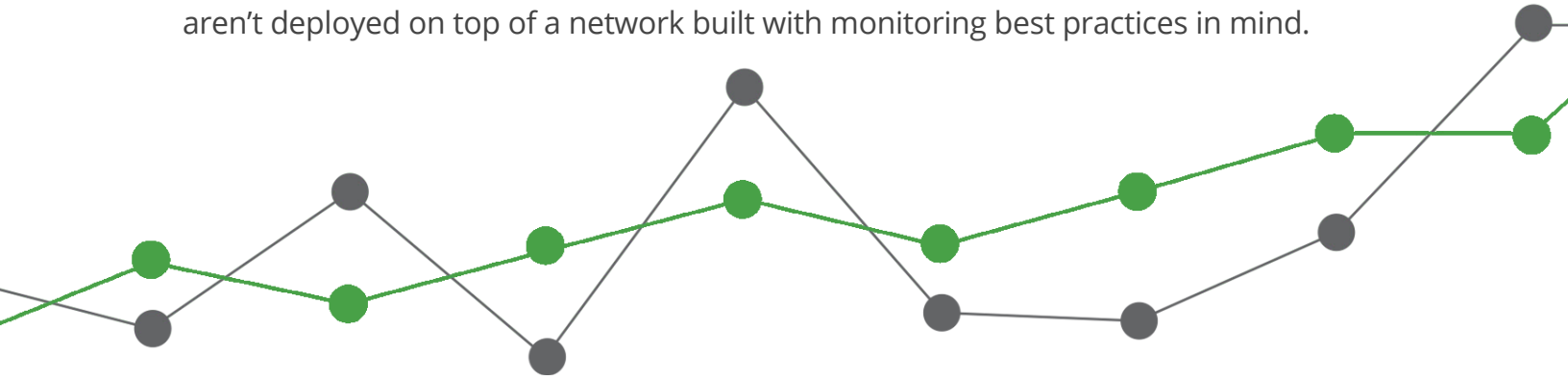
Network monitoring is the collection and analysis of network management information.

Network monitoring encompasses the processes, tools, and software involved in overseeing network operations. This means ensuring availability, tracking overall performance of network services, and maintaining visibility into network access, routers, under-performing components, firewalls, switches, network data, and more.

For years networks have been the lifeblood of business as mission-critical processes become increasingly reliant on connectivity. Network monitoring efforts help admins and IT leaders optimize processes and resources. The ability to perform targeted troubleshooting is important, but being able to proactively identify network bottlenecks and adjust infrastructure strategies accordingly is the ultimate benefit.

One major challenge of network monitoring is that the best strategies are supported by a multitude of tools and applications. Most network monitoring plans include forensics, network analyzers, intrusion detection systems, lawful intercept applications, security information and event management (SIEM) systems, application performance monitoring (APM), deep packet inspection, and more.

As tech teams evaluate the pros and cons of individual tools and applications, it's important to recognize that these products won't work to their fullest potential if they aren't deployed on top of a network built with monitoring best practices in mind.



Putting Network Monitoring Techniques in Place

Before networking professionals get too deep into monitoring discussions, baselining should be the first priority. Taking baseline readings of network traffic is the first step for any network to efficiently spot anomalies later on.

Without a proper network traffic baseline, monitoring efforts will fall short because they won't have anything to compare packet analyses to. There are three key components of the baselining conversation:

1. IP Address Access: Network monitoring strategies should begin with a basic IP scan to see which outside addresses are permitted to talk to the network. With this baseline information, suspicious addresses can quickly be identified before problems occur.

2. Balance of Traffic: Both external and internal traffic should be monitored to get a baseline understanding of what the typical balance looks like so anomalies can be spotted later.

3. Peaks vs. Normal Conditions: Every network has its peak hours for traffic. Knowing the on and off times for the network make it clearer when there's a problem with resource utilization.

While baselining should be the first network monitoring technique deployed, admins need a go-to tool for analyzing packets against this initial data. Enter Wireshark. We'll get deeper into the Wireshark story later in this guide.

11 Key Monitoring Filters

Packet Pioneer Chris Greer recently examined the 11 key filters admins should know about before going any further in network monitoring:

ip.addr == 10.0.0.1
Classic filter for any packet with 10.0.0.1 as source or destination IP.

ip.addr eq 10.0.0.1 and ip.addr eq 192.168.1.1
A conversation filter between two IP addresses.

ip.addr == 10.0.0.0/24
This subnet filter displays conversations to/from any IP within 10.0.0.0/24

tcp or dns
Filter all packets containing TCP and DNS.

tcp.analysis.flags
Display all packets with TCP warnings, including retransmissions, duplicate acks, window updates, and out-of-orders.

tcp contains facebook
Show all TCP packets containing "facebook" (or whichever clear-text string you include in the filter).

http.request or http.response
Display all HTTP request strings and their response codes. HTTP 500 and 404 responses indicate problems.

http.time > 2
Find all HTTP responses sent more than 2 seconds after a request, giving insight into performance.

!(arp or dns or icmp)
This filter blocks arp, dns, icmp or other protocols that could hide a network issue.

tcp.stream eq o
Display all packets in the TCP conversation as well as the packet content (if not encrypted).

sip or rtp
View all sip control and rtp frames in the network trace.

Software-Defined Networking and Cloud Monitoring Concerns

The rapid rise of cloud infrastructure offers the clearest example of how tech leaders can lose track of how important network monitoring really is. As IT leaders scrambled to support increasingly complex business demands for agility and connectivity, network monitoring was left stagnant.

Rather than making incremental upgrades to the network monitoring infrastructure, tech teams went all-in on public cloud providers like Amazon Web Services and Microsoft Azure. The public cloud introduces incredible opportunities for business success—but only if network performance and availability are unhindered.

In response to concerns that network monitoring was falling behind public cloud technology, Amazon Web Services (AWS) released its CloudWatch service. The CloudWatch monitoring dashboard helps IT teams track key network metrics, collect log files, set custom alerts, and react to discrepancies against baseline traffic. The only problem is that self-reported AWS data doesn't cover the entire span of a typical enterprise network. Network monitoring requires more granular, packet-level data to properly assess performance and availability.

For many tech teams, the answer to these cloud-based network monitoring challenges is software-defined networking (SDN); however since SDN can be a large and complicated project to undertake, it may not be the solution for everyone.

This is because while SDN replicates the functions of switches and load balancers, it can't replace network monitoring tools. SDN simply changes the way data is passed from the physical network to applications with separated control and data planes.

The real challenge is maintaining a visibility plane while SDN enables faster and faster network speeds. Rather than trying to push a 1G traditional network to 10G limits, SDN adds agility and flexibility necessary to reach 40G and 100G speeds.

As long as tech teams understand that SDN isn't a replacement for monitoring, they can focus on laying the groundwork for visibility that will eliminate network monitoring headaches as speeds and data streams grow.

Monitoring the Network at 10G, 25G, 40G, and 100G

The networking industry is wholly focused on migration to faster network speeds. Even a few years ago 10G felt out of reach for many, but business demands and tech innovation have put 25G, 40G, and 100G within reach.

Despite the buzz around high-speed networking, many businesses still rely on 10/100/1000M copper Ethernet and legacy network systems. In a perfect world, the shift to network monitoring at 10G, 25G, 40G, and 100G would be simple. However, there are plenty of key decisions to make along the way.

When it comes time to upgrade the network to 10G and beyond, fiber will be required. However, speed is only one factor—media matching and connectivity are the essential considerations that dictate network monitoring success at such high speeds.

Up to 10G speeds, SR, LR, and ER fiber cables can support networking needs. However, when 25G, 40G, and 100G speeds come into play, multi-mode SC and LC fiber connectors have proven inefficient for network monitoring demands. Instead, MTP® brand MPO connectors offer superior stability for continuous visibility.

When media and connectors are chosen, the only question left for high-speed network monitoring is how to get the data from your network to your monitoring tools. When laying the foundation for long-term network monitoring success, the following types of network TAPs will help adhere to infrastructure best practices:

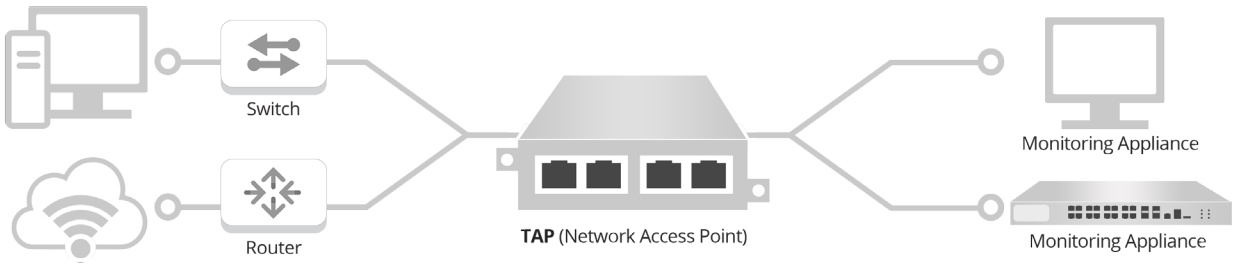
Breakout: is used when utilization is very high and ensure no packets are lost in transmission, as the monitor ports cannot be oversubscribed. This breaks out eastbound and westbound traffic to seperate monitoring ports feeding high-priority monitoring tools.

Filter: When resource utilization is more of a concern, filtering TAPs let admins set rules for what data is sent to monitoring tools. This helps prevent oversubscribed ports.

Aggregator: For high-speed networks on a budget, aggregation TAPs merge traffic streams into one monitoring port to reduce appliance costs. These are powerful solutions when combined with filtering TAPs.

Media Conversion: Whole network refreshes aren't realistic for many businesses. During a transition, network speeds can vary across the organization. Media changing TAPs help normalize connectivity between the network and appliances built for different speeds.

In a later section, we'll dig deeper into the decision to use network TAPs for appliance connectivity as opposed to SPAN ports.



Network Monitoring Tools

As more network devices are used to build bigger networks, network monitoring techniques and tools are expanding. Understanding each application and how they work individually and as a whole is imperative. Here is an overview of the most common monitoring tools and applications.

Forensic

A network forensics tool captures, records, and analyzes network events in order to discover the source of security attacks or other problem incidents.

Application performance monitoring (APM)

An APM monitors and manages the performance and availability of software applications. Making sure the applications perform as expected, optimizing end user experience, runtime application architecture discovery modeling and display, user-defined transaction profiling, component deep-dive monitoring in application context, and analytics.

Network Analyzers

A network analyzer (protocol, packet analyzer or sniffer) can intercept and log traffic and is used to protect against malicious activity by providing activity statistics, bandwidth utilization, detecting unusual levels of network traffic or unusual packet characteristics, and more. Network analyzers can supplement firewalls, anti-virus programs, and spyware detection programs.

Intrusion Detection Systems

An IDS gathers and analyzes information from various areas within a network to identify possible malicious activity or policy violations, which include both intrusions (attacks from outside) and misuse (attacks from within).

Deep Packet Inspection

Deep packet inspection (complete packet inspection and information extraction or IX) a form of packet filtering is a method of analysis that dissects network data to extract useful metadata. Including, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria to decide whether the packet may pass or if it needs to be routed to a different destination.

Network Monitoring Tools

Lawful intercept

Lawful intercept (LI) is a process of obtaining network data pursuant to lawful authority for the purpose of analysis or evidence. Such data generally consist of signaling or network management information, or the content of the communications. If the data is not obtained in real-time, the activity is referred to as access to retained data (RD).

Packet injection

Packet injection is used for troubleshooting network related issues by simulating specific network traffic and scenarios and can be used in testing of network firewalls and intrusion detection systems.

Packet Capture

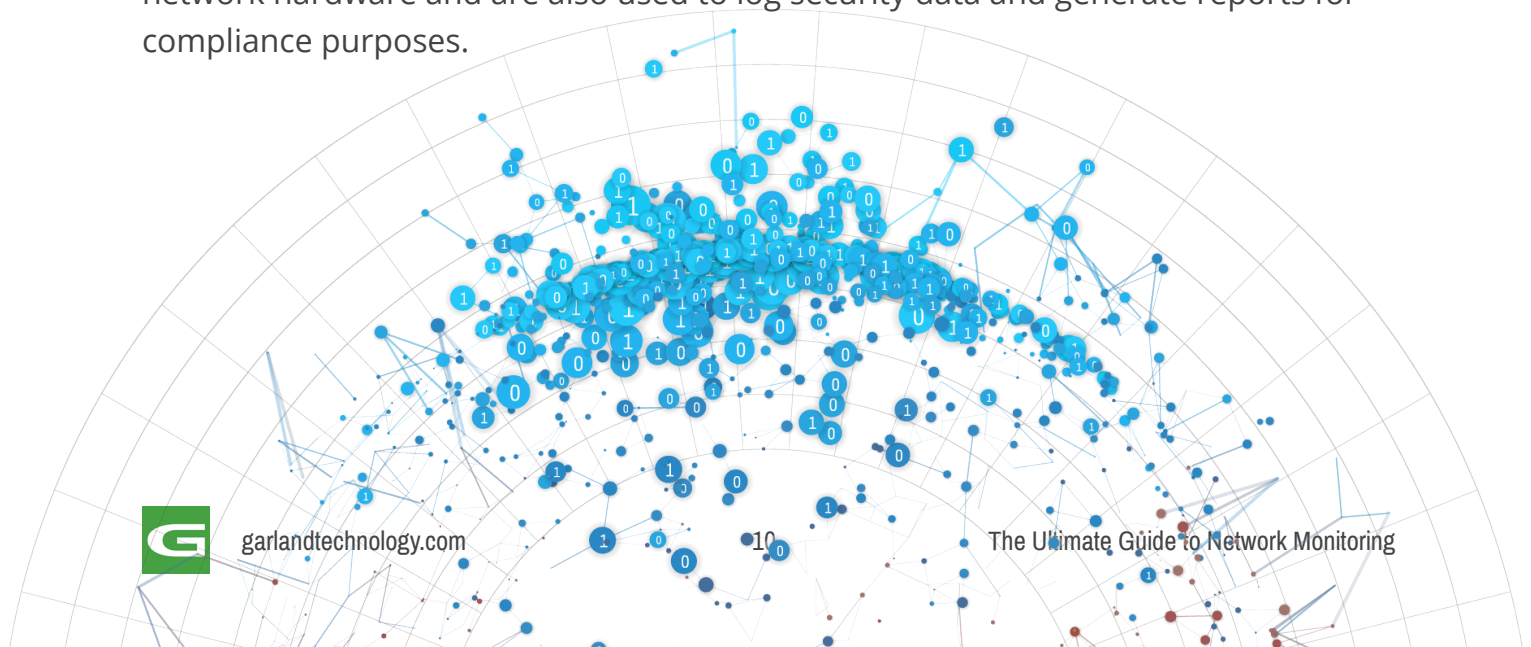
A Packet Capture application captures, logs and examines real-time data packets over a network. Once a packet is captured, it is stored temporarily so that it can be analyzed. The packet is inspected to help diagnose and solve network problems and determine whether network security policies are being followed.

Content Filtering

Content Filtering offers restricted access to only a set portion of a network on an opt-in or a mandatory basis. These filters can be used to implement government, regulatory or parental control over subscribers.

Security Information and Event Management (SIEM)

SIEM provides real-time analysis of security alerts generated by applications and network hardware and are also used to log security data and generate reports for compliance purposes.



Wireshark—The Premier Network Monitoring Tool

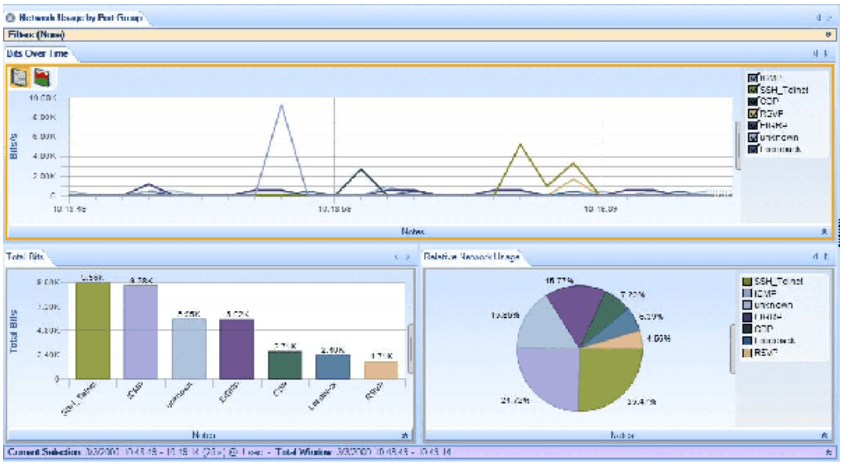
Over the last 20 years, Wireshark has become synonymous with all network monitoring efforts. As a free, open source packet analyzer used for network troubleshooting, analysis and communications protocol development there's no wonder it is an industry standard. However, Wireshark wasn't always Wireshark.

The tool first launched as Ethereal in 1998 with a mission of providing a packet capture device for visually solving network issues. Looking at the story of Gerald Combs, creator of Ethereal, it's interesting to note that the tools was originally written with Solaris and Linux in mind—and complete disregard for Windows. However, as the tool gained traction, Combs recognized significant friction in Windows-based network monitoring, ported the tool to Microsoft's operating system, and saw usage skyrocket.

In the early days of Ethereal, some users saw it as a convenient tool for trace file translation. Networking pros soon realized it was a viable replacement for expensive network analyzers of the early 2000s.

By the time Ethereal became Wireshark in 2006, the tool's features extended beyond its packet/data analyzer roots with:

- A SysDig events analyzer
- Metadata views
- And a growing library of integrations for new methods of data, packet, frame, and merged system information capturing.



All these years later, it's great to look at the differences between Ethereal's interface and today's Wireshark interface and see how network monitoring has evolved.

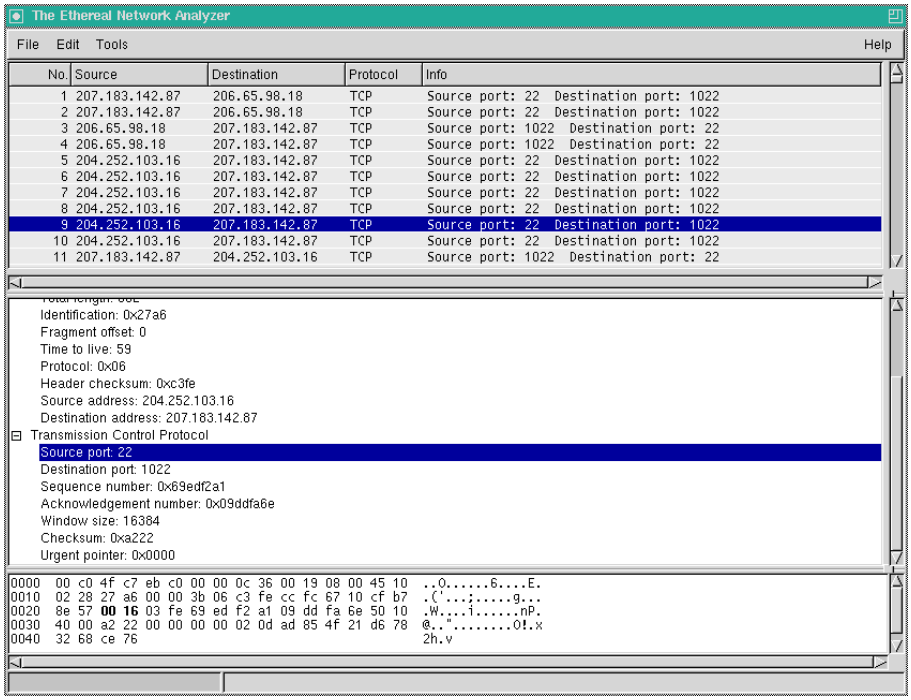


Figure 1: The original Ethereal main capture console with 4 decodes

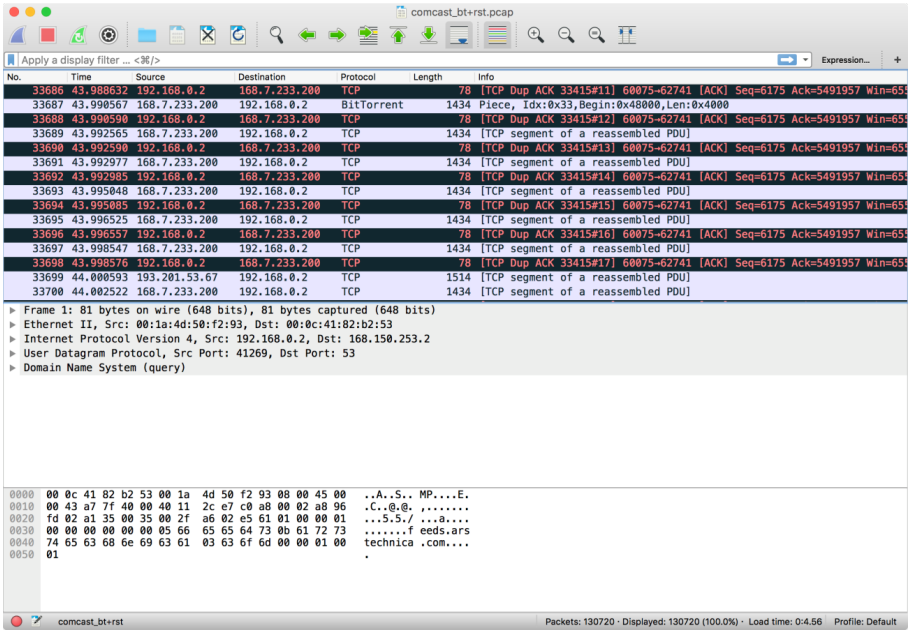


Figure 2: Today's Wireshark with 4000+ Decodes, Including WiFi

TAPs vs. SPAN Ports in Network Monitoring

As switches evolved and improved alongside growing network demands, the utilization of SPAN ports (switch ports for analysis) emerged as a means of mirroring ports to support monitoring efforts.

Instead of connecting to the network directly, engineers could use SPAN ports and direct packets from switches and routers to test devices for analysis. Over the years, networking professionals have grown accustomed to using SPAN ports for monitoring because they are easily accessible—but in best practice, network TAPs have always been the only way to guarantee 100% packet visibility.

Consider the following differences between network TAPs and SPAN ports for network monitoring scalability:

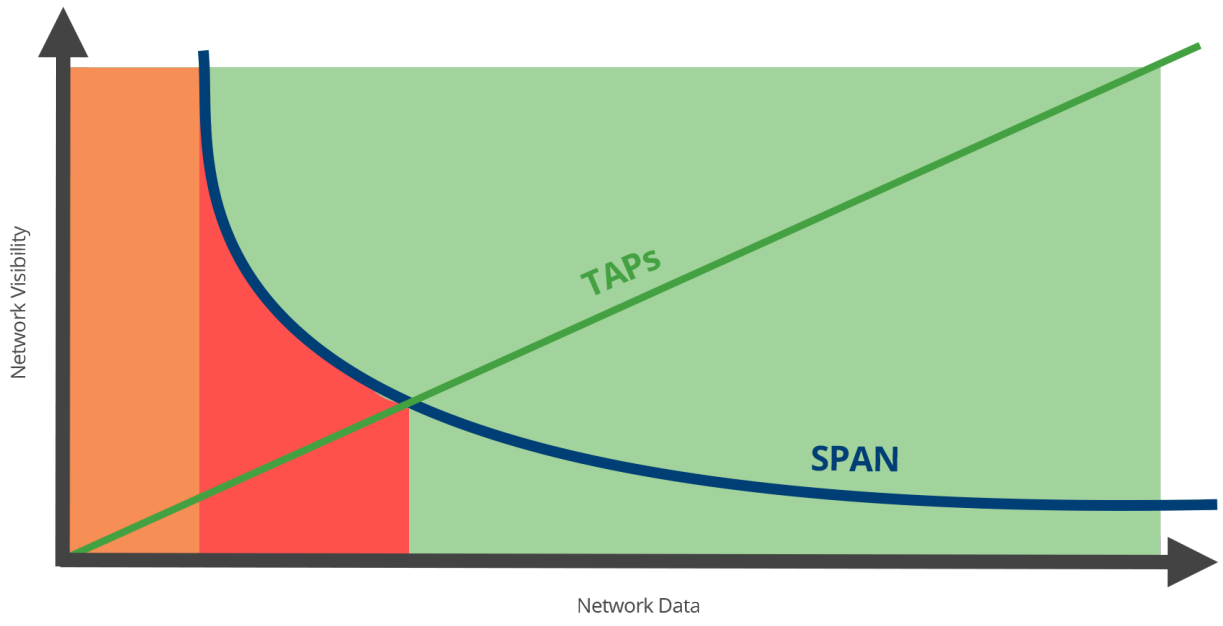


Diagram 3: As your network performance increases, your SPAN port performance is automatically going to decrease and start dropping packets. A network TAP gives100% visibility no matter the network data increase.

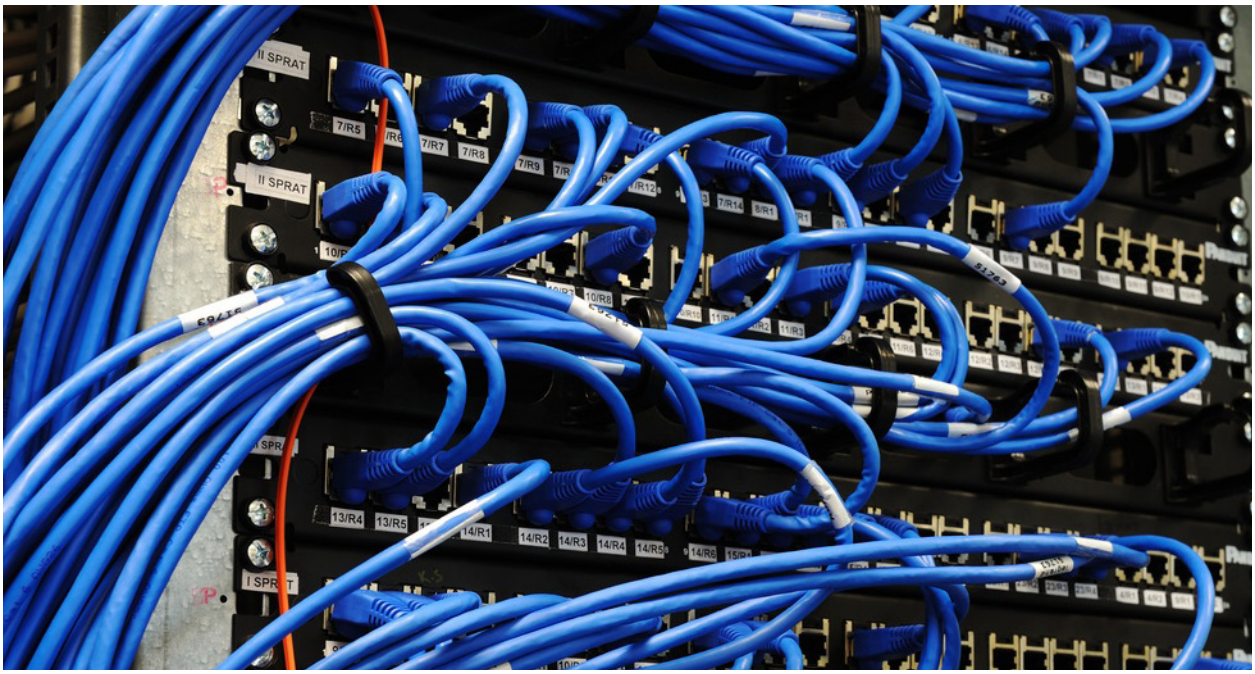
What are the real differences?

Network TAPs transmit send and receive data streams simultaneously on separate, dedicated channels, enabling:

- Passive, listen-only ability to send all data to monitoring tools
- Active, in-line capabilities to feed security tools in real time while providing connectivity failsafe
- Packet capture that doesn't distort or drop data regardless of bandwidth management or physical layer errors
- Real-time communication without altering frame timing, spacing, or responses
- Plug-and-play connectivity that provides 24/7/365 access to 100% of network data

Port mirroring, aka SPAN, sends copies of network packets seen on one port (or a VLAN) to another port where packets can be analyzed, resulting in:

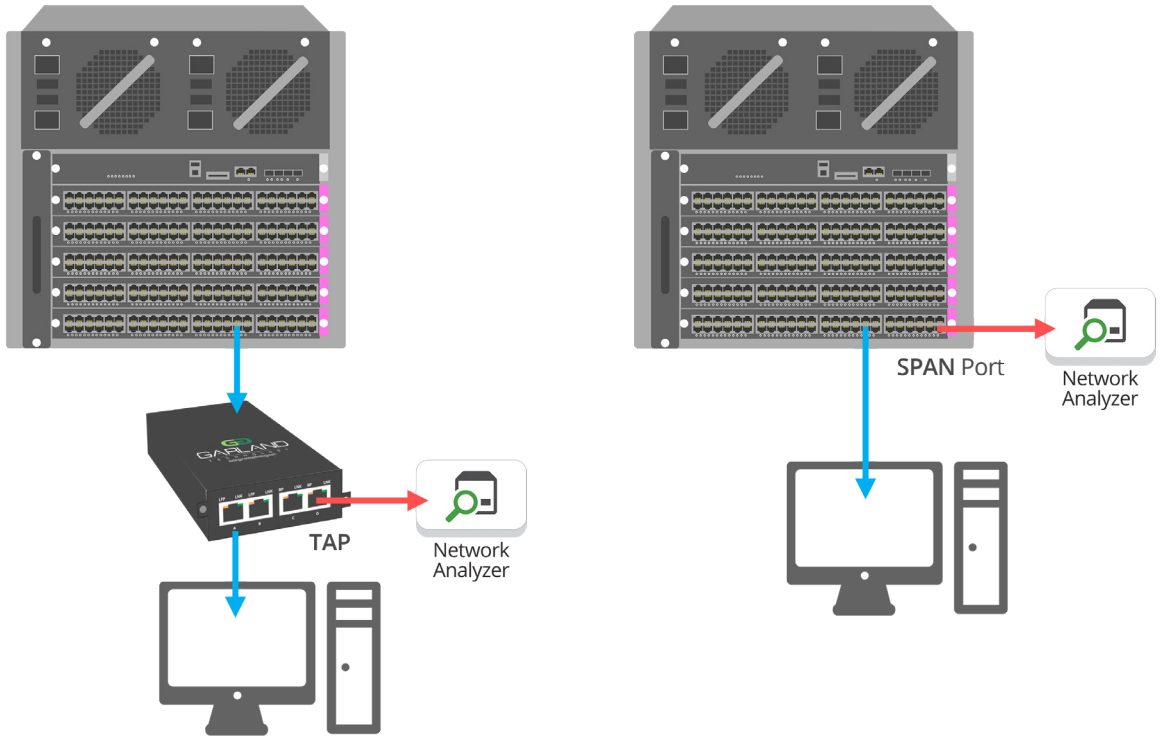
- Single port monitoring
- Packet dropping when ports are oversubscribed
- Distorted real-time communications for applications like VoIP calls
- Degraded performance due to use of production switches and routers
- Easily-misconfigured ports that lead to data loss



Test & Results

Network TAPs are a clear advantage for network monitoring connectivity beyond low-throughput situations. But if advantages and disadvantages aren't enough to persuade networking pros, perhaps practical results will be.

In a recent analysis, Packet Pioneer Chris Greer tested the difference. He connected two PCs to a basic Cisco Catalyst Switch at 100Mbps. A throughput test using iPerf was configured and run between the two machines. On one of the PCs, they placed a 100Mbps TAP, and placed a hardware analyzer on it to capture packets. Lastly, they configured a SPAN on the switch to forward all traffic to and from this port to another hardware analyzer. The throughput test finished with a result of 93.1Mbps sustained for 10 seconds between the two PCs.



TAP Capture Results	SPAN Capture Results
Packets captured: 133,126	Packets captured: 125,221
Delta Time at TCP Setup: 243 uSec	Delta time of TCP connection setup: 221 uSec

Network Monitoring Can't Replace Application Performance Monitoring

In the first section of this guide, we defined network monitoring as the systems/tools put in place to monitor and analyze traffic via packets sent over the network. In theory, one might think that this continuous monitoring would negate the need for application performance monitoring (APM). However, APM and network monitoring are better together.

Network monitoring tools and techniques are meant to gather network metrics like response times and route analytics, all to provide insights into the network infrastructure. Thinking about it from an OSI Model perspective, network monitoring is meant to cover all layers, not dig deep into specific applications.

Application performance monitoring, on the other hand, provides visibility into specific applications by monitoring end-user experience, tracing code-level activity, and feeding into big data analytics. These solutions don't just leave networking pros to recreate ghost issues—they provide granular insights into root causes of performance issues.

Without APM in place, network monitoring tools and techniques will only get IT teams as far as recognizing a problem somewhere in the infrastructure. The amount of lost productivity chasing these problems is more than any business can afford in today's fast-paced business world. Having APM focused on the application layer and network monitoring covering the other layers gives networking pros the power to proactively optimize performance.

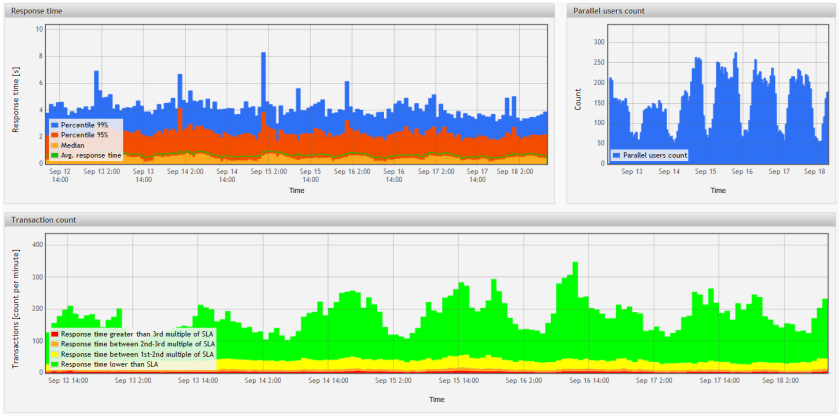


Diagram 4: Application Performance Monitor (APM) by Flowmon, monitors your business critical applications.

Conclusion

Setting Yourself Up for Network Monitoring Success

If there's one main takeaway from *The Ultimate Guide to Network Monitoring*, it's that there is much more to network monitoring than simply deploying a new appliance.

It would be great if there was a network monitoring shortcut. However, networking pros must accept the fact that monitoring requires a ground-up strategy that incorporates best practices at the infrastructure, software, and operational levels.

The key is to implement the right foundation of visibility to support network monitoring efforts for the long haul (even when networks continue to speed up and resource demands grow exponentially). If you want to learn more, visit **Garland's Monitoring Solutions** where we explore common issues like limited data center space, cost effective packet brokers, 100% Packet Capture and 100G Monitoring in SDN.

Want to learn how we can help you implement network monitoring best practices? **Book a free Design-IT** meeting and one of our engineers will work directly with you on designing your network monitoring strategy.

Garland Technology is all about connections – connecting your network to your appliance, connecting your data to your IT team, and reconnecting you to your core business. It's all about better network design.

Garland Technology is a Network TAP (test access point) manufacturer, providing 100% network visibility, anytime network access and zero failures in the field. Seeing every bit, byte and packet is critical. Garland's unique educational-based approach provides your team with the best monitoring and security solutions to meet your needs. Find your solution at: garlandtechnology.com

Contact

Inquiries: sales@garlandtechnology.com

New York | Texas | Germany | UK

GARLAND TECHNOLOGY

See every bit, byte, and packet®

Credit - Chris Greer Network Analyst for Packet Pioneer LLC and Certified Wireshark Network Analyst.

Credit - Tim O'Neill - The "Oldcommguy™"